Maximisez votre sécurité

WatchGuard®

INTRODUCTION

Votre journée commence peut-être par une tasse de café bien chaud (ou un thé si vous n'aimez pas le café) et une longue liste de tâches qui requièrent votre attention immédiate. Vous tentez tant bien que mal d'examiner les alertes de la nuit passée avant que quelqu'un ne se manifeste et que vous ne soyez dépassé par de nouvelles urgences à traiter tout au long de la journée.

Et ce projet sur lequel vous essayez de travailler depuis 3 semaines ? Eh bien, il devra attendre une journée de plus. Ne serait-ce pas une bonne nouvelle si votre solution de sécurité pouvait garantir la sécurité de votre entreprise, vous offrir la visibilité nécessaire sur votre réseau et vous laisser vous consacrer à vos activités quotidiennes ?

Jetez un œil aux menaces de sécurité susceptibles de vous atteindre, aux bonnes pratiques à mettre en œuvre pour les éloigner et à la façon dont WatchGuard peut vous aider.

Mots de passe trop faibles ou réutilisés

81 % des fuites liées à un piratage sont la conséquence d'un mot de passe volé ou trop faible.[1] Il est grand temps d'abandonner les post-its collés sur l'écran de votre ordinateur et les mots de passe du style « 123 ».

Vos employés doivent disposer de mots de passe sécurisés qui peuvent être gérés de manière infaillible. Comment s'assurer que les mots de passe ne rendent pas votre entreprise vulnérable à la fuite de données ?

1 http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Meilleures pratiques relatives au mot de passe

Choisissez un mot de passe SMART

Symboles, lettres et chiffres

Minimum 12 caractères

Abstenez-vous d'utiliser vos informations personnelles

Évitez de réutiliser vos anciens mots de passe

Tirez profit d'outils de gestion de mots de passe

L'authentification multifacteur (MFA)

Les outils de MFA fournissent une preuve d'identité supplémentaire au-delà du simple mot de passe. Ils demandent à l'utilisateur de s'authentifier à l'aide de quelque chose qu'ils connaissent (ex. : un mot de passe), mais également de quelque chose qu'ils possèdent et d'un attribut physique. Cette technique limite la capacité d'un cyber-criminel à utiliser des identifiants volés pour accéder à des comptes.

WatchGuard AuthPoint

Notre solution d'authentification multifacteur unique permet de réduire les risques d'intrusion sur le réseau et de fuites de données en cas d'identifiants perdus ou trop faibles. Elle est par ailleurs hébergée dans le Cloud pour une configuration et une gestion simplifiées et ce, même en cas de ressources restreintes.

« J'ai oublié mon mot de passe »

À l'heure actuelle, les employés ont une multitude de mots de passe à gérer.

En réalité, un employé d'entreprise manipule en moyenne **191 mots de passe** et s'authentifie plus de **150 fois par mois sur des sites Web et autres applications.** Mais vous savez le pire ? **250 employés** d'une entreprise moyenne utilisent à eux tous au bas mot pratiquement **48 000 mots de passe**.[2]

Rien d'étonnant à ce que vos employés oublient leurs mots de passe et demandent leur réinitialisation en permanence !

2 https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

Outils de stockage des mots de passe

Les outils de gestion et de stockage des mots de passe permettent aux utilisateurs d'utiliser des mots de passe très sécurisés sans devoir les mémoriser ! Il est en outre possible de configurer des rappels lorsque les mots de passe doivent être modifiés.

L'authentification multifacteur

Les outils de MFA fournissent une preuve d'identité supplémentaire au-delà du simple mot de passe. Ils demandent à l'utilisateur de s'authentifier à l'aide de quelque chose qu'ils connaissent (ex. : un mot de passe), mais également de quelque chose qu'ils possèdent et d'un attribut physique. Cette technique limite la capacité d'un cyber-criminel à utiliser des identifiants volés pour accéder à des comptes.

En intégrant des solutions de MFA à l'ensemble des ressources numériques d'une entreprise et en offrant aux utilisateurs un accès rapide à un portail d'identification, les utilisateurs n'ont besoin de s'identifier qu'une seule fois et ne doivent plus mémoriser de multiples mots de passe.

WatchGuard AuthPoint

La solution AuthPoint de WatchGuard prend en charge des dizaines d'intégrations tierces au sein d'un écosystème en pleine croissance - vous pourrez ainsi intégrer la protection MFA de WatchGuard à l'ensemble de vos précieuses ressources. Encore mieux, les utilisateurs d'AuthPoint n'ont besoin de s'authentifier qu'une seule fois sur les applications Cloud pour avoir accès à l'ensemble des applications et des ressources Cloud dont ils peuvent avoir besoin dans le cadre de leur travail.

Cliquer sans réfléchir

90 % des attaques commencent par un e-mail d'hameçonnage.[3]

Tant qu'il existera au sein des organisations des personnes qui cliquent sur un lien sans réfléchir , les pirates informatiques continueront à exploiter cette méthode pour diffuser des malwares.

Une formation sur la tactique que représente l'hameçonnage est une bonne manière de sensibiliser l'ensemble de vos employés à la reconnaissance des caractéristiques d'une telle attaque, mais vous devez également posséder une protection contre l'hameçonnage.

L'idéal est même d'être protégé ET d'être formé !

3 https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

Formation sur l'hameçonnage

La formation est essentielle pour enseigner aux utilisateurs les risques inhérents aux e-mails d'hameçonnage et les signaux d'alerte à ne pas manquer. Vous voulez être certain que vos employés sont prêts à se défendre contre toute attaque pénétrant dans leur boîte de réception ?

Surveillance et blocage des DNS

Une formation ne peut protéger à elle toute seule vos employés. Dans la mesure où les e-mails d'hameçonnage deviennent de plus en personnalisés et ciblés, l'ouverture d'un lien malveillant n'est plus qu'une question de temps. Il est donc nécessaire d'implémenter une solution contrôlant le trafic DNS et bloquant l'accès aux sites malveillants.

DNSWatch

DNSWatch de WatchGuard détecte les demandes DNS malveillantes et bloque l'accès aux sites qui redirigent les utilisateurs vers une page sécurisée les sensibilisant aux risques et aux signes permettant d'identifier les tentatives d'hameçonnage. Ces événements sont des « moments d'information » pour vos employés et constituent un moyen efficace de leur enseigner les risques inhérents au hameçonnage.

Les téléchargements de fichiers malveillants

À l'instar des liens malveillants par e-mail, l'envoi de pièces jointes malveillantes par e-mail représente une autre méthode couramment utilisée par les pirates informatiques pour déployer leurs attaques.

Cette méthode consiste pour les pirates informatiques à inciter leurs victimes à télécharger une pièce jointe bien spécifique.

Parmi les types de pièces jointes malveillantes figurent :

- les factures
- les documents numérisés
- les notifications d'échec de l'envoi d'un e-mail
- les confirmations de commande et de paiement
- les confirmations de trajets spécifiques

Pouvez-vous protéger vos utilisateurs contre ce type d'attaques malveillantes ?

La protection contre les menaces basée sur les signatures

L'analyse des fichiers malveillants connus avant même leur ouverture offre le niveau de détection nécessaire pour prévenir cette méthode d'attaque.

La sandbox dans le Cloud pour disséquer les fichiers

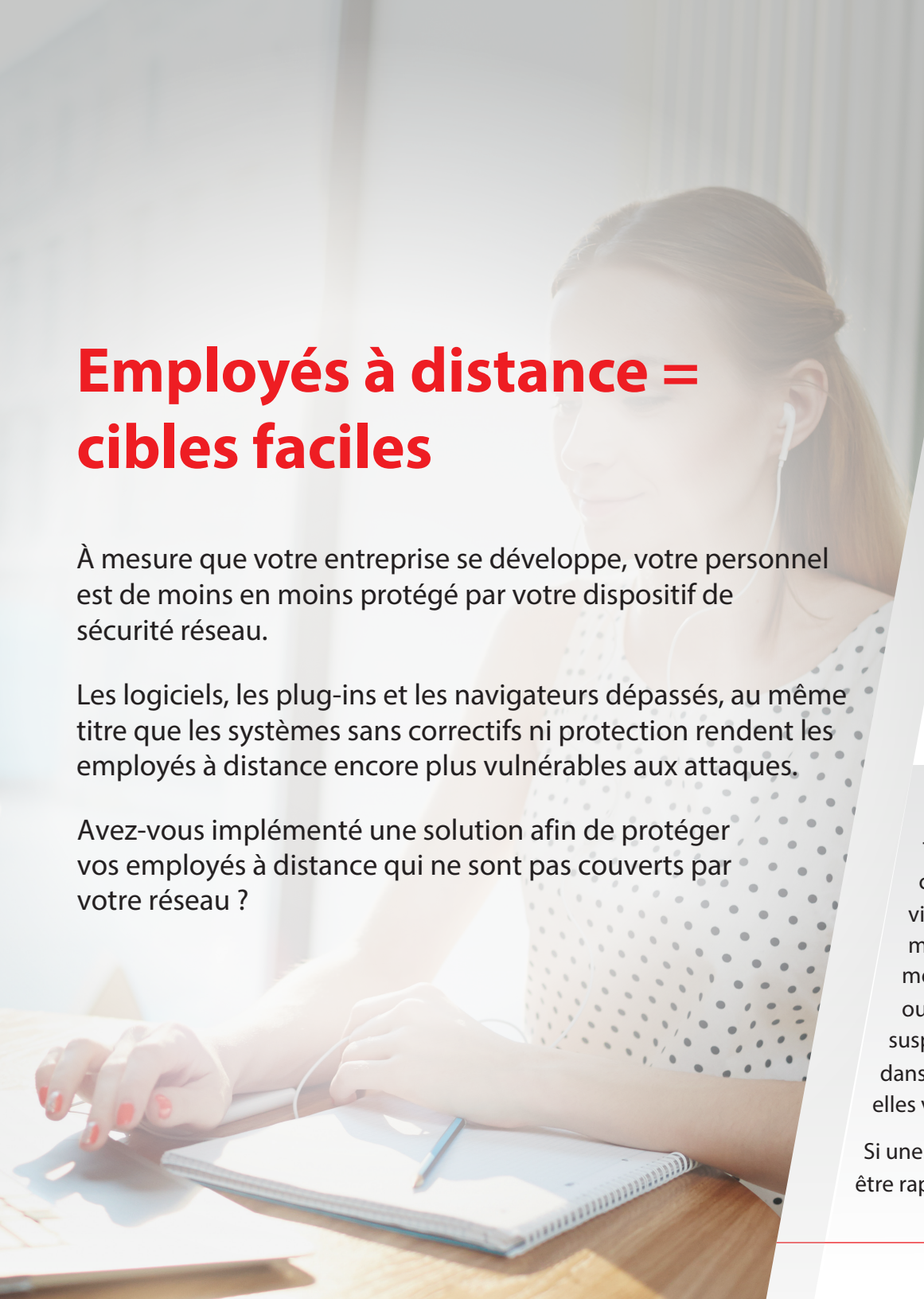
La sandbox dans le Cloud est un moyen sécurisé de détecter de nouvelles menaces et de détruire les fichiers potentiellement malveillants. En les ouvrant dans un environnement virtuel qui reflète votre système, vous pouvez avoir un aperçu clair du contenu malveillant sans faire courir de risques à votre appareil.

GAV et APT Blocker

Inclus dans la Total Security Suite de WatchGuard, le Gateway AntiVirus (GAV, antivirus de passerelle) et l'APT Blocker offrent plusieurs couches de défense contre les pièces jointes malveillantes véiculées par les attaques par hameçonnage.

Le GAV garantit la mise à jour continue de la base de données de signatures afin de bloquer l'ouverture des pièces jointes malveillantes.

Les menaces inconnues et les attaques de malware de type Zero Day impliquent quant à elles toute une série de nouveaux défis en termes de sécurité. Toutefois, grâce à l'APT Blocker de WatchGuard, ces fichiers sont disséqués dans un environnement virtuel sécurisé afin de déterminer s'ils possèdent un contenu malveillant. Si tel est le cas, le fichier sera mis en quarantaine afin de veiller à ce qu'il ne soit pas ouvert.



Employés à distance = cibles faciles

À mesure que votre entreprise se développe, votre personnel est de moins en moins protégé par votre dispositif de sécurité réseau.

Les logiciels, les plug-ins et les navigateurs dépassés, au même titre que les systèmes sans correctifs ni protection rendent les employés à distance encore plus vulnérables aux attaques.

Avez-vous implémenté une solution afin de protéger vos employés à distance qui ne sont pas couverts par votre réseau ?

Analyse de menaces approfondie

Il est nécessaire d'implémenter de solides solutions de protection pour combattre les menaces avancées et évasives. Il existe une façon de se protéger contre ces menaces : les outils d'analyse de menaces approfondie tels que la sandbox pour les réseaux et les hôtes. En disséquant les menaces malveillantes et suspectes dans un environnement virtuel sécurisé, vous pouvez consulter le contenu d'une menace avant qu'elle n'affecte vos utilisateurs.

Visibilité élargie jusqu'au poste de travail

Vous ne pouvez bloquer ce que vous ne voyez pas. Ainsi, pour les employés à distance, vous devez avoir de la visibilité sur les postes de travail, même lorsqu'ils ne sont pas connectés au réseau.

TDR et agent Host Sensor

Threat Detection and Response (TDR), qui inclut le capteur WatchGuard Host Sensor, offre une visibilité accrue sur les événements et les activités menaçant les postes de travail de vos utilisateurs, même lorsqu'ils ne sont pas connectés au réseau. En outre, TDR permet de disséquer les menaces suspectes susceptibles d'affecter le poste de travail dans un environnement virtuel afin de déterminer si elles véhiculent un quelconque contenu malveillant.

Si une menace est jugée malveillante, elle peut être rapidement éliminée avant tout incident.

La navigation des employés & le faible débit

Le fait de consulter des sites chronophages ou inappropriés peut exercer un impact considérable sur la productivité de votre entreprise.

L'employé moyen perdrait plus de 8 heures par semaine dans des activités qui ne concernent pas son emploi. Soit une journée de travail complète ![4]

En cas de faible débit, c'est votre activité même qui peut être ralentie. Est-ce la faute de vos employés qui regardent trop de vidéos sur YouTube ? Ou peut-être est-ce un employé qui regarde le match auquel il n'a pas pu assister ?

Comment pouvez-vous faire en sorte que vos employés maximisent leur productivité au bureau et, plus important encore, qu'ils ne consultent pas de sites Web dangereux ou inappropriés sur leur lieu de travail ?

4 https://nypost.com/2017/07/29/this-is-how-much-time-employees-spend-slacking-off

La visibilité sur l'activité Internet

Vos employés doivent avoir accès à Internet dans le cadre de leurs fonctions, mais cette activité peut également affecter les performances de votre réseau. Vous avez besoin d'une bonne visibilité sur la navigation des utilisateurs afin de déterminer si le problème provient de l'accès à des sites chronophages par exemple.

Filtrage des URL

Vous devez être en mesure de protéger votre réseau contre le contenu Web risqué, les activités malveillantes et les sites chronophages. Le filtrage des URL vous permet de mettre en œuvre une stratégie d'entreprise afin de veiller à ce que l'accès à tous ces sites soit contrôlé et approuvé.

WebBlocker

WatchGuard WebBlocker offre une solution puissante et simple d'utilisation pour le contrôle et la surveillance de l'activité Internet au sein de votre entreprise. En outre, vous pouvez facilement bloquer ou limiter les activités non professionnelles afin de veiller à ce qu'une bande passante adéquate soit disponible en permanence.

Dimension

WatchGuard Dimension vous permet de consulter l'activité réseau en temps réel présentée au sein de tableaux de bord et de rapports intuitifs et interactifs. Vous pouvez ainsi voir qui consomme le plus de bande passante, s'il existe des modèles de trafic inhabituels et quels sites Web sont le plus souvent visités.

Quelle sera la prochaine menace majeure ?

Vous n'avez pas le temps (ou simplement pas l'énergie) de rester au fait des tendances en matière de menaces et d'attaques de malwares actuelles.

Pourtant, les menaces continuent d'évoluer et les pirates informatiques attaquent votre entreprise de tous les côtés.

Avez-vous implémenté une solution afin de vous protéger contre les menaces de malwares connues, inconnues et évasives ?

Accès à la recherche sur les menaces de manière simple

Même lorsque vous n'avez pas le temps, vous devez rester au fait des tendances et des prévisions en matière de menaces. Si ne possédez pas la bande passante pour le faire vous-même, assurez-vous de travailler avec des équipes qui peuvent le faire pour vous.

Une sécurité par couches pour une protection à tous les niveaux

Les attaques d'aujourd'hui et les menaces de demain nécessitent des solutions de sécurité impliquant plusieurs couches. Vous devez avoir la capacité de vous défendre contre chaque type d'attaque à tous les niveaux.

Total Security Suite

Total Security Suite de WatchGuard offre une protection contre les menaces avancées à chaque niveau. Des services fondamentaux tels que Gateway AntiVirus ou le Service de prévention d'intrusions jusqu'à des services plus avancés tels que la sandbox dans le Cloud ou encore la prévention des pertes de données, WatchGuard a toujours une solution à proposer afin de vous protéger contre les menaces connues, inconnues et évasives.

Le paysage des menaces

Notre équipe de recherche sur les menaces poursuit un objectif clé – rester informée des tendances en matière de menaces et des dernières attaques afin que vous ne deviez pas le faire vous-même. Nous entendons vous informer sur les tendances en la matière et vous prodiguer des conseils avisés afin de vous protéger contre les dernières menaces.

Vous êtes débordé en raison d'alertes constantes ?

Vous êtes constamment sur la brèche ?

La protection de votre bureau ne doit pas mobiliser tout votre temps – il vous suffit d'implémenter les bonnes solutions de sécurité.

Vous avez besoin d'une solution qui protège votre entreprise à tous les niveaux.

La protection de votre entreprise doit être assurée 24 heures sur 24, 7 jours sur 7 et 365 jours par an. Cela ne signifie pas pour autant que vous ne puissiez pas vivre votre vie.

Vous avez besoin de visibilité sur l'activité réseau et les événements relatifs aux menaces tout en vous sentant rassuré, car vous êtes protégé contre les attaques à chaque niveau de votre réseau.

WatchGuard

WatchGuard offre à ses clients une solution de sécurité intelligente et facile d'utilisation. Total Security Suite offre une protection contre les menaces connues, inconnues et évasives au sein d'une solution simple d'utilisation. Muni d'une appliance et d'une licence, vous pouvez disposer des services de sécurité nécessaires au prix qui vous convient.

WatchGuard Dimension, qui est fourni en standard avec nos appliances, fournit une suite d'outils de visibilité « big data » et de génération de rapports qui permettent d'identifier et d extraire instantanément les tendances, menaces et autres problèmes majeurs susceptibles d'affecter la sécurité de votre réseau.

Trouvez l'appliance WatchGuard la plus adaptée à votre entreprise !
Pour de plus amples informations, veuillez consulter le site https://www.watchguard.com/compare

PROTÉGEZ VOTRE ENTREPRISE • PROTÉGEZ VOS RESSOURCES • PROTÉGEZ VOS COLLABORATEURS

Jamais la cyber-sécurité n'a été aussi primordiale. Le nombre de cyber-attaques dans le monde entier a atteint des sommets sans précédent, et rien ne permet de dire que cela va diminuer. Les TPE, PME, ETI et administrations sont de plus en plus ciblées, et les conséquences sur leur activité sont de plus en plus graves. WatchGuard offre la protection multicouche dont vous avez besoin pour contrer les malwares les plus avancés et ce, en toute simplicité. Vous êtes confronté aux mêmes menaces que les grandes entreprises. Pourquoi ne pourriez-vous pas bénéficier du même niveau de sécurité ?

Siège social mondial
États-Unis
Tél. : +1 800 734 9905
E-mail : sales@watchguard.com

Bureaux français

Tél : +33 (0)1 40 90 30 35
E-mail : france@watchguard.com

Siège social APAC et SEA
Singapour
Tél. : +65 3163 3992
E-mail : inquiry.sea@watchguard.com

WatchGuard®

© 2018 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard, AuthPoint, DNSWatch, Dimension et Firebox sont des marques commerciales ou des marques déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs détenteurs respectifs. Référence WGCE67101_080718